'적이 노릴 만한 나의 정보' 실시간 파악 및 관리

위협 인텔리전스 기반 공격 표면 관리 자동화 서비스

powered by Criminal IP

KLU:ASM

IGLOO

Background

조직을 둘러싼 IT 환경이 급격히 변화함에 따라, 공격자가 노릴만한 공격 표면(Attack Surface)은 점점 더 넓어지고 있습니다.
이에 오늘날의 IT/보안 담당자들은 방대한 네트워크에 걸쳐 노출된 수많은 주요 자산을 신속히 파악·조치해야 하는 막중한 과제에 직면하고 있습니다.

IT/보안 담당자가 관리해야하는 수많은 주요 자산

DB 서버	원격 콘솔 서버	그룹웨어 서버
API 키	개발 서버	VPN 익스플로잇

이것이 바로 공격 대상이 될 수 있는 주요 자산 노출 여부를 미리 파악·관리해 공격 가능성을 사전에 최소화하는
'공격 표면 관리(ASM)' 도입이 필요한 이유입니다.

Overview

'공격 표면 관리(Attack Surface Management)'는 해커가 침투할 수 있는 열린 Port와 각종 서버 취약점, 유사 도메인과 피싱, 악성코드 유포 도메인 등의 공격 표면을 미리 탐지하고 관리하는 것입니다. '클루 에이에스엠(KLU: ASM)'은 전 세계 네트워크에 흩어져 있는 조직의 수많은 IT 자산을 실시간으로 확인 및 조치할 수 있게 지원하는 위협 인텔리전스 기반 공격 표면 관리 서비스입니다.

조직의 운용 자산 중 단 한 개의 대표 도메인 등록을 통해, 시시각각 변화하는 IT 자산 현황에 대한 자동 식별 및 공격 표면 관리가 가능합니다.

KLU: ASM

New Assets
추가되거나 변경된 자산
자동 탐지

IP Assets
탐지된 IP 주소의
열린 포트를 스캔하여 제공

Domain / Certificate
등록된 도메인의 서브 도메인과
적용된 인증서 정보 제공

OSINT (Google Hacking)
구글에 노출된 민감한 정보,
서버, 파일 탐지 제공

Risk
IP, 도메인, 인증서, 어플리케이션 등
공격 가능한 모든 자산의 취약점 제공

Intelligence Search Result
자산의 공격표면 노출 정보와
취약점 상세 정보 확인

Dashboard
전체 자산 통계와 자산 위치 정보,
취약점 현황과 그래프를 대시보드로 제공

Report
새로운 자산 탐지 및 취약점에 대한
공격 표면 관리 리포트를
자동 생성하여 정기적으로 제공

Why KLU: ASM

① 고객 자산 자동 탐지

· 고객이 알고 있는 자산과 알지 못하는 자산까지 전체 인터넷 대상으로 스캔
· 사용중인 IP 주소와 열려 있는 모든 Port에서 운용 중인 네트워크 자산 전체를 탐지

IP	Port	Domain
42억 개 IP 주소 정보	전 세계 Port 스캔 데이터	3억 개 이상의 Domain 주소 데이터

IP Address · Domain · TCP · UDP · Application · SSL Certificate · RDP · Webcam · IoT · SCADA · ICS · DNS Record · NNTPS · NTP · MySQL · Bitcoin · Printer · CCTV · Firewall · QNAP · Cloud Server · Darkweb · Proxy · TFTP · Default Password · Name Server · VPN

② 자산 및 취약점 위험도 스코어링

· AI 머신러닝을 통한 자체 알고리즘을 통해 실시간 탐지된 모든 자산을 5단계의 위협 스코어링으로 시각화
· 보안 담당자는 시각화된 스코어링을 통해 사이버 위협 우선순위를 지정하여 빠르고 정확하게 보안 위협에 대응

	IP/Asset	Domain/Certificate
Critical	네트워크 및 자산에 공격의 흔적이 있거나 공격 당하고 있는 상태	도메인과 인증서가 위조되었거나 악성 링크가 포함되어 위험한 상태
Dangerous	네트워크 및 자산이 공격표면에 노출되어 공격 될 수 있는 상태	도메인이 위조되었거나 인증서가 유출 또는 만료되어 관리가 필요한 상태
Moderate	네트워크 및 자산이 일반적인 보안 정도를 유지하고 있는 상태	도메인과 인증서가 일반적인 보안 정도를 유지하고 있는 상태
Low	네트워크 및 자산이 외부에 노출되어 있지 않고 안전한 상태	도메인이 위조되었거나 인증서가 유출, 만료되지 않은 안전한 상태
Safe		

Why KLU: ASM

③ 위협 인텔리전스 검색엔진 및 AI 탐지 모델 서비스 연동

사이버 위협 인텔리전스 KLU: Threat Intelligence 검색엔진과 연동

· Search, Intelligence, API 통합 기능을 추가적으로 사용 가능
· 최신 글로벌 보안 위협에 대한 일일 분석 리포트와 통계로 보안 동향을 파악해 더 효과적인 공격 표면 관리 가능

위협 인텔리전스 검색엔진 주요 기능

Search	Intelligence
Asset Search	Banner Explorer
Domain Search	Vulnerability
Image Search	Statistics
Certificate Search	Element Analysis
Exploit Search	Map

분류형·설명형·생성형 AI 탐지 모델 서비스 AiR와 연동

· Payload 분석 서비스 및 ChatGPT 연계 자연어 설명 제공
· 빅데이터 리포트 및 인텔리전스 리포트 제공 (개발 중)

AiR AI Road

IGLOO 탐지모델	AI 학습데이터에 대한 학습을 통해 보안 관련 이상·정상 행위 등을 분류하는 기술
설명가능한 AI	AI가 어떤 기준에 따라 특정 행위를 이상·정상으로 탐지 했는지를 알려주는 기술
생성형 AI 챗GPT	기존 콘텐츠에 대한 학습을 토대로 새로운 콘텐츠를 만들어내는 AI 기술

④ 클라우드 기반 웹 인터페이스

· KLU: ASM은 SaaS 형태의 ASM 제품으로 도입 시 고객사 서버 내에 하드웨어 또는 소프트웨어를 설치하거나 구축할 필요가 없음
· 고객사 계정 등록 이후 고객사의 네트워크가 연결된 PC, 태블릿, 모바일 기기의 브라우저를 통해 웹 인터페이스로 빠르고 쉽게 공격표면관리 솔루션 사용

설치형
On-Premises

· 초기 제품 설치 및 내부 서버 구축
· 시스템 업데이트 패치, 업그레이드
· 내부 서버 및 네트워크 장애 이슈 관리
· 하드웨어 유지보수 및 업그레이드
· 네트워크 유지보수 및 업그레이드
· 보안 유지보수 및 업그레이드
· 데이터베이스 유지보수 및 업그레이드

클라우드
SaaS

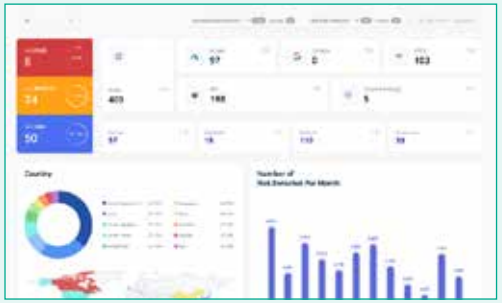
- 연간 구매
- 사용법 가이드 및 교육
- 맞춤형 커스터마이징

Features

단 한 개의 도메인 제공으로, 연결된 모든 IT 자산을 둘러싼 잠재 위협 가시성을 확보할 수 있습니다.
전 세계 IP 정보 기반의 사용 정보, 위험등급을 제공합니다. 또한 간단한 검색으로 악성 URL 및 도메인 검증, 노출된 취약점 정보를 파악할 수 있습니다.

Dashboard

자동 탐지된 자산의 위협 인텔리전스 정보를 대시보드로 시각화합니다. 위험도에 따라 High, Medium, Low 3 단계로 구분하여 보안 조치가 시급한 자산을 빠르게 파악할 수 있습니다.



IP Assets (Application)

등록된 IP 자산의 요약된 정보(위험도 Score, AS Name, 위치 정보, 취약점)를 확인할 수 있습니다. IP 주소를 클릭하면 사이버 위협 인텔리전스 KLU: Threat Intelligence 검색엔진으로 연동되어, IP 주소에 대한 위협 인텔리전스를 조회할 수 있습니다.

Risk

사용자가 등록한 자산(IP, Domain)의 공격 가능한 위협 벡터가 발견되면 자동으로 RISK 페이지에 추가되어 위협에 노출된 자산 정보를 확인할 수 있습니다.

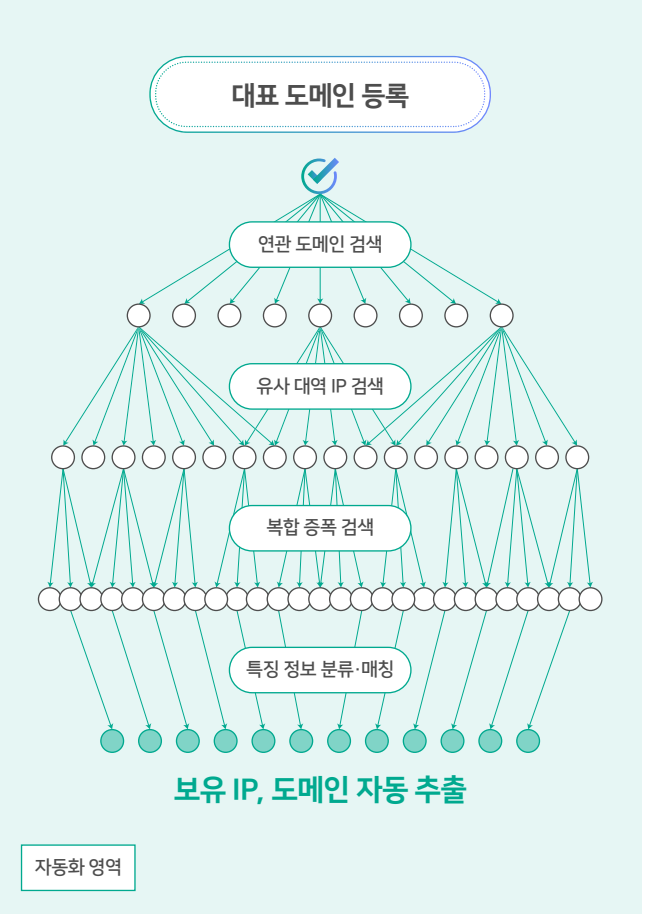
Domain / Certificate

등록한 도메인의 요약된 정보(Score, Technology, jQuery, PHP 등)와 도메인에 대한 취약점 개수(Vuln.), 인증서 정보(SSL, Encryption, SSL Expire Date), 서브 도메인에 대한 요약 정보를 보여줍니다.

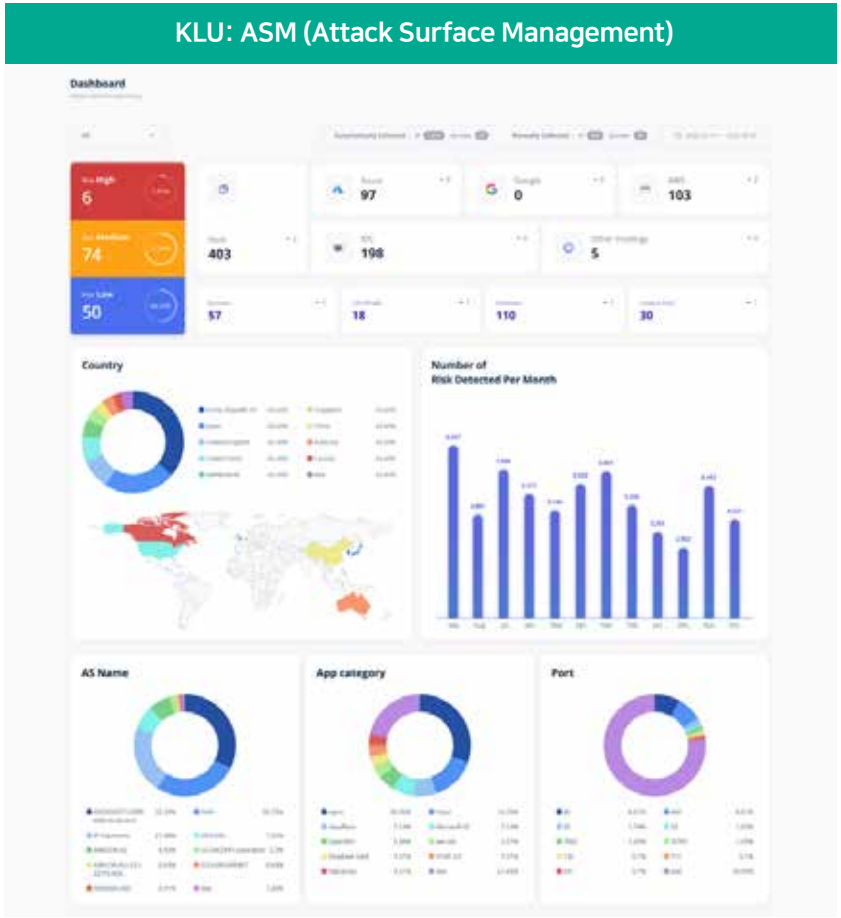
Features

KLU: ASM 도입에는 오직 한 가지, 대표 도메인 주소만 필요합니다.

운용하고 있는 자산 중 대표 도메인 등록을 통해, 공격 표면 관리 가능하여 고객의 편의성을 증대해줍니다. 전 세계 네트워크에 분포되어 있는 모든 자산을 자동으로 식별하여 공격 표면 관리 자동화가 가능합니다.



자동 등록



Benefits

KLU: ASM 도입으로 '적이 노릴 만한 내 정보'를 간편하고 정확하게 파악하세요.

전 세계 네트워크에 흩어져 있는 조직의 IT 자산을 실시간으로 확인하고, 문제점을 신속히 조치함으로써, 고도화된 공격에 대한 방어력을 한 단계 높일 수 있습니다.
또한 시시각각 변화하는 IT 자산 현황에 대한 자동 식별 및 IP·도메인·인증서·애플리케이션 등 자산 취약점을 확인할 수 있습니다.

- 공격 표면 침투 확률 감소
- 비용 & 리소스 절감

- 업무효율 증가
- 공격 표면 보안성 향상

KLU: ASM 도입 예시

새로운 취약점이 발견된 경우

기업이 운용 중인 자산에 대한 위협 인텔리전스 분석을 통해
공격 가능한 취약점이 있는 자산의 경우,
위협 스코어링으로 시각화 하여 리포트를 제공합니다.

1. KLU: ASM — KLU: ASM 도입
   KLU: ASM을 통한 상시 취약점 점검 실행
2. Log4j — 취약점 발생
   대규모 보안 취약점(Log4shell) 이슈 발생
3. 자동 점검
   KLU: ASM으로 취약점 (Log4shell) 보유한 자산 전체 점검
4. 즉각 대응
   대응프로세스에 따라 취약점 리포트 확인 및 즉각 대응 조치

상,하반기 대규모 취약점 점검 해제
KLU: ASM으로 자동 리포트 보고

위험한 포트가 오픈되는 경우

열려 있으면 안되는 포트가 실수로 오픈 되었거나,
오픈된 채로 방치된 경우, KLU: ASM이 실시간으로
모든 IP의 포트를 스캔하여 위협 리포트를 제공합니다.

1. KLU: ASM — KLU: ASM 도입
   KLU: ASM을 통한 실시간 포트 및 운용자산 스캔
2. 포트 감지
   외부 접근 제한된 오픈 포트 및 자산 다수 발견
3. 즉각 대응
   ASM 자동 리포트로 확인 후 포트 폐쇄 및 즉각 대응 조치

KLU: ASM으로
실시간 운용 포트 및 자산 관제

새로운 자산이 추가되는 경우

외부에 노출된 채로 방치되어 있거나 파악하지 못하고 있는
자산을 KLU: ASM의 실시간 자산 스캐닝을 통해
파악할 수 있습니다.

1. KLU: ASM — KLU: ASM 도입
   KLU: ASM을 통한 사이버 자산 실시간 자동 탐지
2. 미확인 자산 발견
   알리바바 클라우드에 미확인 자산 발견
3. 즉각 대응
   ASM 자동 리포트로 확인 후 서버 삭제 및 즉각 대응 조치

미사용 중인 이벤트 페이지 폐쇄 및
KLU: ASM으로 클라우드 자산 관리 자동화

1999년 보안 벤처 기업으로 시작한 이글루코퍼레이션은 국내 최초 보안 정보 및 이벤트 관리(SIEM) 솔루션을 시작으로 수많은 정보보호 핵심 중추 기관과 기업에 보안 솔루션 및 서비스를 제공하며 정보보안 시장의 성장을 이끌어왔습니다. 또한, 디지털 전환 시대 흐름에 맞는 꾸준한 기술 고도화 및 미래 기술 준비를 통해 사업 영역을 확장해 나가며 보안을 넘어 인공지능, 클라우드, 빅데이터 분야를 아우르는 종합 IT 기업으로 성장했습니다. 이글루코퍼레이션은 세계의 고객에게 고유의 보안과 데이터 역량에 기반한 최적의 솔루션, 서비스를 제공하며 급변하는 비즈니스 환경에 최적화된 혁신적인 디지털 경험을 선사하는 기업으로 나아가고자 합니다.

서울특별시 송파구 정의로8길 7 한스빌딩 6층 | TEL 02-3452-8814 | FAX 02-3452-8815 | www.igloo.co.kr

IGLOO